CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

ANÁLISE JURÍDICA E SOCIAL DO ESTELIONATO VIRTUAL: DESAFIOS, LEGISLAÇÃO E MEDIDAS DE PROTEÇÃO

Renam da Paz Eller

Presidente Prudente/SP

2024

CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

ANÁLISE JURÍDICA E SOCIAL DO ESTELIONATO VIRTUAL: DESAFIOS, LEGISLAÇÃO E MEDIDAS DE PROTEÇÃO

Renam da Paz Eller

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação do Prof. Mario Coimbra.

Presidente Prudente/SP

2024

ANÁLISE JURÍDICA E SOCIAL DO ESTELIONATO VIRTUAL: DESAFIOS, LEGISLAÇÃO E MEDIDAS DE PROTEÇÃO

Monografia aprovada como requisito parcial para obtenção do Grau de Bacharel em Direito.

Mario Coimbra

Carla Roberta Ferreira Destro

Florestan Rodrigo do Prado

Presidente Prudente/SP

2024

Dedico essa pesquisa a todas as pessoas vítimas do estelionato virtual e que elas possam se atentar aos métodos de prevenção para o delito.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado a oportunidade de apresentar esse trabalho com um tema que é recorrente no cenário atual e assim enriquecendo meu intelecto. Por ter me dado sabedoria para finalizar e concluir a monografia com maestria.

A minha família, em especial aos meus pais, pois graças aos seus esforços posso estar concluindo minha graduação.

Ao meu orientador Mario Coimbra, por ter me orientado ao longo desse período tirando todas as dúvidas que tive e demonstrado eficiência no tema mencionado. Aos examinadores Florestan Rodrigo do Prado e Carla Roberta Ferreira Destro por conferir a oportunidade de apresentar minha pesquisa diante de profissionais exemplares e pelas aulas expostas na graduação que me ajudaram a enriquecer o corpo do texto mencionado na pesquisa.

Por fim aos professores e coordenadores do curso de Direito do Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente, por todos os ensinamentos ministrados no decorrer da minha graduação, bem como ao restante dos funcionários da faculdade, pelas inestimáveis contribuições.

RESUMO

A monografia fundamentou-se em explanar sobre o delito de estelionato virtual no Brasil, baseando-se em referências bibliográficas. Nesse sentido, foi mencionado no primeiro capítulo a respeito do crime de estelionato na legislação brasileira e seu desenvolvimento durante a história do país. Ainda no primeiro capítulo, foi relatado sobre a classificação do crime, destrinchando e detalhando sobre o delito previsto no artigo 171 do Código Penal Brasileiro. Já no segundo capítulo, foi apresentado a fraude eletrônica e as suas discussões que estão muito presentes no cotidiano atual. Foi mencionado a respeito das modalidades mais praticadas pelos criminosos e métodos para se prevenir e não se configurar como vítima do crime. Por fim, foi abordado o tema do direito comparado, ou seja, o delito de estelionato visto de modo internacional, mostrando como os países estão lidando com esse tipo de infração.

Palavras-chave: Estelionato Virtual; Legislação Brasileira; Código Penal; Modalidades; Métodos; Direito Comparado.

ABSTRACT

The monograph was based on explaining the crime of virtual fraud in Brazil, based on bibliographic references. In this sense, it was mentioned in the first chapter regarding the crime of embezzlement in Brazilian legislation and its development during the country's history. Still in the first chapter, the classification of the crime was reported, unraveling and detailing the offense provided for in article 171 of the Brazilian Penal Code. In the second chapter, electronic fraud and its discussions were presented, which are very present in today's daily life. It was mentioned about the modalities most practiced by criminals and methods to prevent themselves and not become victims of crime. Finally, the topic of comparative law was addressed, that is, the crime of fraud seen internationally, showing how countries are dealing with this type of infraction.

Keywords: Virtual Fraud; Brazilian Legislation; Penal Code; Modalities; Methods; Comparative Law.

SUMÁRIO

1 INTRODUÇÃO

No cenário contemporâneo, a prática do estelionato apresenta um desafio social e jurídico de relevância imensurável. Trata-se de um delito que ultrapassa limites geográficos e sociais, afetando não apenas pessoas físicas, mas também empresas e instituições governamentais.

Se valendo do método dedutivo e pesquisas bibliográficas é possível perceber que o crime de estelionato sempre esteve presente em nossa sociedade, desde as épocas mais arcaicas, e é introduzido no Código Penal no capítulo em que se trata dos crimes contra o patrimônio, onde traz como definição que o estelionato é a obtenção para si ou para outrem vantagem ilícita, induzindo ou mantendo alguém à erro. O delito está elencado no caput do artigo 171 do Decreto-Lei nº 2.484 de 07 de setembro de 1940 (Código Penal Brasileiro), em seu capítulo VI, onde trata de outras fraudes além dos estelionatos.

No entanto, com a evolução da informática surgiram diversos meios que facilitaram a realização de atividades no cotidiano da população. Entretanto, algumas pessoas más intencionadas utilizaram dessa evolução para aplicar fraudes com o intuito de obter alguma vantagem, normalmente pecuniária, em relação a algum terceiro.

Diante desse cenário, a pesquisa não abordou somente a evolução histórica do delito e suas classificações, mas menciona detalhadamente a respeito do ponto de vista do direito digital, abordando princípios fundamentais do Marco Civil da internet que regularizam e ajudam a prevenir que esse crime venha a se consumar. Apresenta também, uma análise ampla das modalidades que os criminosos utilizam para obter uma certa vantagem ilícita sobre as vítimas e como se prevenir deste crime.

2 O DELITO DE ESTELIONATO NA LEGISLAÇÃO BRASILEIRA

Até o surgimento das normas autônomas brasileiras, o país se utilizava das ordenações filipinas, que com grande influência portuguesa tipificava o estelionato como “burla” da mesma forma que Portugal naquela época.

O primeiro Código Penal do Brasil, mais conhecido como Código do Império, elaborado em 1830, trazia uma distinção entre os escravos e os cidadãos livre no momento de aplicar as sanções, ainda que os crimes fossem praticados da mesma maneira, violando o princípio da igualdade. O próprio Código permitia que os juízes sentenciassem os cidadãos livre a diversas penas distinta a depender do crime como: morte na forca, galés (trabalhos públicos forçados com indivíduos acorrentados uns aos outros), prisão com ou sem trabalho, banimento (expulsão definitiva do Brasil), pagamento de multa e suspensão ou demissão do trabalho. Dessa imensa lista de sanções, apenas a morte e galés eram aplicadas aos povos escravizados e caso recebessem uma pena mais branda, esta era convertida automaticamente em açoites – pena que era proibida aos povos livres. Posteriormente a pena de morte era aplicada somente para três delitos: homicídio com certos agravantes, latrocínio e liderança de insurreição escrava.

Foi no Código do Império que o delito de estelionato surgiu com esse *nomem juris* e estava elencado no artigo 264 onde seus quatro parágrafos traziam expressamente os requisitos para que os indivíduos fossem enquadrados no respectivo artigo.

> Art. 264. Julgar-se-ha crime de estellionato:
> 1º A alheação de bens alheios como proprios, ou a troca das cousas, que se deverem entregar por outras diversas.
> 2º A alheação, locação, aforamento, ou arretamento da cousa propria já alheiada, locada, aforada, ou arretada á outrem; ou a alheiação da cousa propria especialmente hypothecada á terceiro.
> 3º A hypotheca especial da mesma cousa á diversas pessoas, não chegando o seu valor para pagamento de todos os credores hypothecarios.
> 4º Em geral todo, e qualquer artificio fraudulento, pelo qual se obtenha de outrem toda a sua fortuna, ou parte della, ou quasquer titulos.
> Penas - de prisão com trabalho por seis mezes a seis annos e de multa de cinco a vinte por cento do valor das cousas, sobre que versar o estellionato.

Assim como no Código do Império de 1830, o Código Penal Republicano de 1890 adotou as mesmas casuísticas tipificando onze figuras de estelionato, incluindo uma modalidade geral que foi conceituada como:

> Usar de artificio para surpreender a boa-fé de outrem, iludir a sua vigilância, ou ganhar-lhe a confiança; induzindo-o em erro ou engano por esses e outros meios astuciosos, procurar para si lucro ou proveito (Bittencourt, 2012, p. 630-634).

Tendo em vista o atual Código Penal, o dispositivo sofreu diversas alterações como pode ser vista em sua redação elencada no artigo 171 do decreto lei nº 2.484/1940:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

Deve ser ressaltado o artigo 5º da Constituição Federal que possui a seguinte redação:

> Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XXII – é garantido o direito de propriedade.
> XXIII – a propriedade atenderá a sua função social.

Diante do exposto no texto constitucional, é direito de todo cidadão a inviolabilidade de seu patrimônio particular. Porém, no cotidiano atual, os infratores estão se aperfeiçoando cada vez mais para que os delitos se concretizem e assim, consigam obter a vantagem sob a pessoa que está em erro.

Também pode ser notado que com o passar dos anos, as sanções para o determinado delito se tornaram cada vez mais severa visando punir os infratores para que estes não voltem a cometer tal conduta.

Para Nelson Hungria (1942, p.11) o que havia antes eram crimes mais violentos e bárbaros, hoje se tem se uma composição entre os delitos mais agressivos que ocorriam no passado, porém tiveram uma evolução a passar para crimes mais engenhosos e planejados.

Tendo em visto os acontecimentos ao decorrer da história global, pode-se concluir que o delito do estelionato se aperfeiçoou e novas modalidades surgiram. Deste modo, cabe ressaltar a intenção dos estelionatários que, na maioria das vezes, é a vantagem pecuniária, situação que infelizmente acontece repentinamente na

sociedade atual e acaba afetando a vida financeira da vítima e da sua respectiva família.

2.1 Evolução histórica do crime de estelionato

O delito do estelionato pode ser considerado por muitos um crime atual ou moderno, porém ele está presente na sociedade desde as épocas arcaicas e até mesmo na Bíblia no livro de Genesis, onde relata que a serpente enganou Eva para que esta comesse do fruto da árvore do jardim do Éden. Tal conduta está meramente relacionada ao crime presente em nosso ordenamento jurídico, que traz como conceito “obter vantagem ilícita, para si ou para outrem, utilizando-se de meios fraudulentos”.

Este delito surgiu ao redor do mundo possuindo terminilogias diferentes, como “frode” no Código Toscano, “trufa” no código de Zanardelli e código Rocco, “estafa” no código espanhol e, “betrug” no código alemão.

Não se sabe ao certo qual foi especificamente o primeiro caso de estelionato, mas um dos primeiros casos registrados do delito teria acontecido em 300 a.C na Grécia Antiga, onde Hegestratos e Zenosthemis, dois mercadores marítimos elaboraram um plano para se enriquecerem através de uma apólice de seguro para o seu navio de carga. O acordo presente na apólice era de que os comerciantes eram obrigados a reembolsar o dinheiro emprestado com juros após a venda de suas mercadorias e caso não conseguissem pagar o empréstimo, o credor obteria a posse do navio e sua respectiva carga. Após saírem em alto mar, Hegestratos tinha o plano de afundar o barco vazio e embolsar o dinheiro que havia sido emprestado e vender a carga que tinha abandonado. Porém o plano falhou e ele tentou fugir e acabou se afogando no mar, enquanto seu parceiro foi pego em flagrante e, posteriormente, julgado pelo tribunal ateniense.

Posteriormente, após 500 anos, ocorreu o primeiro caso de fraude financeira, em Roma, no ano de 193 d.C. Os soldados do imperador o assassinaram e tomaram o poder com fim de vender o império em um leilão. Porém, como o império não pertencia a eles de fato, eles fraudaram o licitante oferecendo algo que eles não tinham a propriedade.

No Código Penal Francês de 1810 em seu artigo 405 estava elencado o delito de estelionato que possuía como descrição a obtenção ou tentativa de obtenção de

vantagem patrimonial, por meio de manobras fraudulentas (Bittencourt, 2023, P. 158). O delito recebeu diversas denominações, mas uma das principais foi “burla”, como era adotada nas Ordenações Filipinas e que, por sua vez, adotou a pena de morte para quem pratica o delito e o prejuízo fosse superior a vinte mil-réis.

Na era do Iluminismo, no século XVII e XVIII, Isaac Newton, foi um dos principais nomes para essa era e foi nomeado Mestre da Casa da Moeda Real. Em seu mandato, ele buscou protegê-la dos falsificadores, conduta que era complexa para aquela época. William Challoner, foi um dos falsificadores mais famosos da história que estimou sua quantia em £ 30.000 (trinta mil libras) em apenas dois anos cometendo o ato ilícito.

Já nos Estados Unidos, no ano de 1792, o presidente George Washington foi vítima de um golpe financeiro que foi praticado por William Duer, que era especulador financeiro conhecido do presidente. Ele utilizou de informações privilegiadas que possuía e se envolveu em um dos primeiros pânicos financeiros do país e, diante disso, foi confinado a prisão dos devedores.

Em 1821, Gregor MacGregor, um soldado escocês, atraiu investidores e colonos britânicos e franceses para um território fictício que este afirmava possuir. Centenas de pessoas investiram sua economia em suposto títulos do governo e certificados de terras e, posteriormente, descobriram que foram fraudados. Este foi considerado o primeiro registro de fraude imobiliária da história.

2.2 Classificação do crime de estelionato

Para que se possa entender mais sobre o delito de estelionato, deve-se levar em consideração a sua classificação mediante a atual legislação brasileira. A classificação do estelionato envolve diversos aspectos, incluindo a natureza dolosa do agente, ou seja, a intenção deliberada de enganar, e a presença de um meio fraudulento para a realização do delito e também outras particularidades como: bem jurídico tutelado, sujeitos, tipo objetivo, tipo subjetivo, entre outros. Além do mais, o estelionato pode ser subdivido em diversas modalidades, dependendo do *modus operandi* utilizado pelo agente infrator, como por exemplo o estelionato eletrônico.

2.2.1 Bem jurídico tutelado

Como o delito está elencado no tópico de “crimes contra o patrimônio”, o bem jurídico a ser tutelado seria a inviolabilidade do patrimônio, mais especificamente em relação aos atentados que podem ser praticados mediante fraude. É tutelado tanto os interesses sociais relacionados a confiança que deve presidir os relacionamentos patrimoniais individuais e comerciais, quanto o interesse público de reprimir a fraude causadora de dano alheio (Bittencourt, 2023, p. 159) e manter a ordem econômica.

A proteção jurídica visa assegurar que as transações e relações patrimoniais se desenrolem em um ambiente de confiança e transparência, extremamente necessário para obter relações sociais e econômicas estáveis.

2.2.2 Sujeito ativo e passivo

Por se tratar de um crime comum, o sujeito ativo do delito pode ser qualquer pessoa, sem qualquer condição especial e, o concurso de pessoas também pode se configurar (Bittencourt, 2023, p.159). Este sujeito é quem induz ou mantém a vítima em erro, empregando algum tipo de meio fraudulento. O legislador quando conceituou o delito mencionou que a “vantagem indevida pode ser para si ou para outrem”. Essa terceira pessoa pode ser considerado coautor ou participe do crime sendo alcançada pelo concurso de pessoas, previsto expressamente no artigo 29 do Código Penal Brasileiro. Mas nada impede que o terceiro beneficiário do produto do estelionato seja um estranho sem qualquer participação na execução ou planejamento do crime, sendo assim, não será passível de qualquer tipo de sanção. Este sujeito é quem induz ou mantém a vítima em erro, empregando algum tipo de meio fraudulento.

O sujeito passivo, por sua vez, também pode ser qualquer pessoa, ou seja, qualquer pessoa pode ser vítima do crime de estelionato. No entanto, pode haver situações em que há mais de um sujeito elencado no polo passivo como por exemplo casos em que o agente use algum meio fraudulento para enganar uma pessoa e está entregue um bem pertencente a outra, hipótese em que ambas são vítimas de um único estelionato (Gonçalves, 2022, p.523). Nesse caso, como destacava Roberto Lyra, “o sujeito passivo da ação, do erro, é quem sofre sua materialidade”, ou seja, a vítima efetiva é aquela que sofre o dano material decorrente da ação.

Para a vítima ser enganada é indispensável que está possua capacidade de discernimento e em casos que a vítima venha a ser uma criança ou um enfermo mental, se leva em consideração que eles não possuem a capacidade de entender e de querer e, assim, não podem ser mantidos em erro e tampouco podem ser sujeitos desse crime. Caso tal situação venha a acontecer o sujeito ativo deve ser enquadrado no delito elencado no artigo 173 do Código Penal Brasileiro que trata a respeito do abuso de incapazes (Baldan, 2017). Portanto, ao enquadrar um sujeito no crime abuso de incapazes assegura uma proteção mais eficaz a indivíduos que não possuem capacidade de discernimento e, assim, não conseguem se defender de práticas fraudulentas.

2.2.3 Ação nuclear

Como foi visto, o estelionato consiste em obter vantagem ilícita, para si ou para outrem, utilizando-se de meios fraudulentos e alguns doutrinadores, como Fernando Capez, trazem um conceito mais técnico a respeito do delito: ‘’consiste em induzir ou manter alguém em erro, mediante o emprego de artificio, ardil ou qualquer meio fraudulento, a fim de obter, para si ou para outrem, vantagem ilícita em prejuízo alheio (Capez, 2024).’’

O estelionato não é um delito em que se utilizar de violência ou grave ameaça para que seja consumado, apenas induz a pessoa e assim comete o delito.

Para que se possa entender mais a respeito do crime, deve-se levar em consideração a ação nuclear, que seria basicamente a expressa do verbo que exprime a conduta do agente, que distingue dos demais delitos. De acordo com o doutrinador Fernando Capez, os meios empregados para a prática do delito são: “artifício” que está relacionado a fraude no sentido material, como relatou Mirabete “ o artificio existe quando se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa”; “ardil” que este, por sua vez, está relacionado a fraude no sentido imaterial, dirigindo-se a inteligência da vítima e objetivando estimular nela uma emoção ou convicção pela criação de uma motivação ilusória e; qualquer outro meio fraudulento: apesar do artificio ser compreendido com uma expressão genérica, vale ressaltar que pode ser utilizado qualquer outro tipo de conduta que venha a enganar ou manter a vítima em erro para que o delito de estelionato se consume.

Deve se analisar também outros aspectos e não somente os meios utilizados, como por exemplo o erro que de acordo com o doutrinador Cezar Roberto Biterncourt “é a falsa representação ou avaliação equivocada da realidade”. Pode ser analisado também, a vantagem ilícita que é o objeto material do delito, no qual o agente emprega meios fraudulentos para iludir a vítima com intuito de obter vantagem ilícita em prejuízo alheio. Se a vantagem for lícita, haverá o crime de exercício arbitrário das próprias razões (Capez, 2024, p. 241). Cumpre ressalvar que o doutrinador Damásio E. de Jesus citou que a vantagem ilícita deve ser econômica, por se tratar de crime patrimonial, portanto essa vantagem deve estar relacionada a vida econômica da vítima. Já o prejuízo alheio é o dano de natureza patrimonial, ou seja, o prejuízo sofrido pela vítima deve ser uma perda patrimonial.

2.2.4 Consumação e tentativa

Por se tratar de crime material a consumação se caracteriza quando o agente atinge o proveito econômico, assim causando danos a vítima (Capez, 2024. P. 242). O delito consuma-se, portanto, no momento e lugar em que o agente obtém o proveito a que corresponde o prejuízo alheio. No crime em si, não basta apenas a existência do erro decorrente da fraude, mas sim que aquele erro resulte em uma vantagem ilícita e prejuízo patrimonial de algum terceiro (Bitencourt, 2023, p. 164) assim então sendo indispensável a presença do prejuízo ilícito sofrido.

Por se tratar de crime material é perfeitamente admissível que seja configurado em sua forma tentada uma vez que a conduta que resultaria na consumação pode ser interrompida por motivos diversos a vontade do agente, como pode ser notado diariamente em casos que os agentes se passam por gerentes de bancos e falam que os usuários devem depositar uma determinada quantia em dinheiro e na hora de efetuar o depósito no caixa eletrônica recebe a informação que o banco não solicita depósito para seus clientes. Tal conduta é divergente caso for comprovada que a fraude que fora tentada ser aplicada era ineficaz, tratando assim de um crime impossível por absoluta ineficácia do meio (Gonçalves, 2022, p. 523) como pode ser mencionada em uma situação hipotética em que um agente se passando por parente entra em contato telefônico solicitando um depósito via PIX e quando a vítima tenta efetuar o pagamento consta que a conta bancária não existe.

2.2.5 Fraude Bilateral

A fraude bilateral ou também chamada de torpeza bilateral acontece quando a vítima também age de má-fé, ou seja, também possui a intenção de obter a vantagem ilícita (Gonçalves, 2020, p. 114) como por exemplo o golpe do bilhete premiado, quando uma vítima acredita que vai se beneficiar pela compra de um bilhete de loteria premiado (por um preço muito menor do que o valor do prêmio a ser recebido), mas, na verdade, o resultado prático será outro.

Há dois entendimentos na doutrina em relação a esse aspecto. O primeiro, de Nelson Hungria, entende que não há estelionato por três motivos: (i) somente goza de proteção legal o patrimônio que serve a um fim legítimo, dentro de sua função econômico-social; (ii) o Código Civil, em seu artigo 883, caput, dispõe que "não terá direito a repetição aquele que deu alguma coisa para obter fim ilícito, imoral, ou proibido por lei". Só existe estelionato quando alguém é iludido em sua boa-fé, logo quando houver má-fé por parte da vítima, falta um pressuposto básico para o crime em si. Já a segunda posição, por sua vez, menciona que existe estelionato, não importando a má-fé do ofendido e é considerada a posição majoritária, que é adotada por alguns doutrinadores como Fernando Capez, Heleno Fragoso, Edgard Magalhaes Noronha, entre outros.

2.2.6 Arrependimento posterior

O doutrinador Cezar Roberto Bitencourt menciona que o arrependimento posterior seria: "uma minorante, aplicável a determinados crimes, praticados sem violência ou grave ameaça à pessoa, quando houver reparação do dano ou restituição da coisa antes do recebimento da denúncia ou da queixa".

Essa reparação do dano não necessariamente precisa ser espontânea, basta que seja voluntária, podendo o agente ser convencido a reparar o dano ou restituir a coisa. Porém, o benefício não será aplicado caso o agente seja obrigado a praticar tal conduta, mesmo que por sentença judicial.

Tal benefício está presente em nosso ordenamento jurídico no artigo 16 do Código Penal que seria uma redução de pena que, como menciona o texto legal, poderá ter, o agente, a pena reduzida de um a dois terços.

Para que se entenda melhor esse benefício deve ser levado em consideração três aspectos: Crime praticado sem violência ou grave ameaça à pessoa que nesse caso, somente está relacionada à pessoa, portanto se a violência ou grave ameaça for contra a coisa, não exclui a minorante; Reparação do dano causado pelo crime ou restituição da coisa que, por sua vez, essa reparação deve ser pessoal, completa, total e voluntária. Caso não esteja presente esses requisitos, tal benefício somente será usado como atenuante e; a reparação ou restituição devem ocorrer antes do recebimento da denúncia ou da queixa que se ocorrer após o recebimento da denúncia ou da queixa, será utilizada apenas como atenuante genérica presente no artigo 65, III, b, in fine, do Código Penal (Fonseca, 1999).

Portanto, infere-se a necessidade de estar presentes os requisitos para que o benefício da diminuição de pena, caso contrário, será apenas enquadrada como atenuante genérica.

2.2.7 Modalidades

O artigo 171 do Código Penal menciona o crime de estelionato, porém pode se notar diversas formas elencadas dentro deste artigo e seus respectivos parágrafos, como estelionato simples, privilegiado, figuradas equiparadas e estelionato eletrônico.

A forma simples é o delito de estelionato em sua forma genérica, como está previsto no caput do artigo 171, caput, do Código Penal, com pena de reclusão de 1 a 5 anos, e multa.

Não obstante, o estelionato privilegiado, previsto no art. 171 em seu parágrafo 1º, menciona que se o criminoso é primário e é de pequeno valor o prejuízo sofrido pela vítima, o juiz pode aplicar a pena conforme o disposto no artigo 155 §2º. Portanto a diferença do delito elencado no art. 155 §2º (furto privilegiado) e o estelionato privilegiado é que no primeiro a coisa furtada deve ser considerada de pequeno valor. Já no estelionato privilegiado, exige-se que seja de pequeno valor o prejuízo sofrido pela vítima, o qual deve ser aferido no momento da consumação do delito. O benefício para determinada conduta é a substituição da pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicara somente a pena de multa. Nesse caso, quando se refere ao poder do juiz de aplicar algum benefício ao autor do crime, surge alguns debates acerca da sua faculdade ou obrigatoriedade.

Para Nucci o magistrado é livre, não podendo ser obrigado a dar interpretação em favor do réu, porém reconhecendo existentes todos os requisitos, é natural que tenha a obrigação de conceder o benefício, pois a lei não deve ser utilizada como objeto de capricho do seu aplicador (Nucci, 2024, p. 413).

Cabe mencionar a respeito das figuras equiparadas estão elencadas nos seis incisos do §3º do mesmo artigo:

> § 2º - Nas mesmas penas incorre quem:
> I - Vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
> II - Vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;
> III - Defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;
> IV - Defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
> V - Destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as consequências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;
> VI - Emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.

O primeiro inciso, refere-se à disposição de coisa alheia como própria, que convém destacar que os mesmos elementos presentes no estelionato em sua modalidade fundamental também estão presentes nessa figura (Bittencourt, 2023, p. 165). Nesse caso, exige-se má-fé do sujeito ativo, ou seja, o estelionatário e correspondente a boa-fé do sujeito passivo.

Já o segundo inciso, menciona a respeito da alienação ou oneração fraudulenta de coisa própria. Nesse caso, o que diferencia esse inciso é o objeto material que no caso de ser coisa alheia, trata-se de coisa própria impedida de ser alienada.

O terceiro inciso, por sua vez, faz menção a defraudação de penhor que acontece quando o devedor pignoratício, que tem a posse do objeto empenhado, defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia. Um exemplo que pode ser mencionado nessa ocasião é a alienação na lavoura de soja constituída em garantia por meio de cédula rural pignoratícia, sem o consentimento do credor.

Não obstante o quarto inciso diz respeito a fraude na entrega da coisa que basicamente é quando o agente tem a obrigação de entregar a coisa ou o bem e não entrega ou entrega parcialmente.

Já o quinto inciso relata sobre a fraude para o recebimento de indenização ou valor de seguro, que nesse caso o bem protegido nessa modalidade é o patrimônio do segurador.

Por fim, o sexto inciso comenta sobre a fraude no pagamento por meio de cheque que foi o último a ser inserido no ordenamento, criado pela lei n. 2591/2012 (Lei do Cheque). Nesse caso foram cominadas as mesmas sanções previstas para o crime de estelionato, para a emissão de cheques sem a correspondência provisão de fundos. As ações de “emitir” e “frustrar” estão presentes nessa modalidade, cujo a primeira tem o sentido de colocar em circulação o cheque sem suficiente provisão de fundos e, a segunda, está relacionada a obstar o pagamento, bloqueando, retirando o saldo existente e, dessa forma, evitar o pagamento do cheque.

2.2.8 Majorantes

No texto legal do artigo 171, mais especificamente em seu parágrafo terceiro e quarto estão previstas as majorantes a respeito do delito. A primeira, presente no parágrafo terceiro relata a respeito do delito cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficiária, cujo a pena aumentará de um terço.

O parágrafo quarto, por sua vez, trata-se de uma causa de aumento de pena especial que as vítimas são os idosos ou vulneráveis. No caso mencionado, a pena aumente de um terço para o dobro. Um caso que pode ser mencionado como exemplo é o da Vara Criminal de Águas Claras que condenou a ré Fabiane do Nascimento Chaves a sete anos, nove meses e dez dias reclusão, em regime semiaberto, pela prática do delito. Neste caso em observação, a ré foi contratada para trabalhar como cuidadora de uma idosa de 74 anos de idade e utilizou de facilidades de convívio e apoderou-se do cartão de crédito da idosa. No período de janeiro a maio de 2017 (cinco meses), a ré gerou um prejuízo para a vítima de R$ 376.521,24 (trezentos e setenta e seis mil, quinhentos e vinte e um reais e vinte e quatro centavos). De acordo com o Ministério Público do Distrito Federal e Territórios

(MPDFT), o autor da respectiva ação, a ré se passava por filha da idosa para justificar os pagamentos com o cartão.

Diante do exposto, vale ressaltar que o exemplo citado é um caso de aumento de pena, uma vez que a pena máxima em abstrata do crime de estelionato comum é de cinco anos, conforme o caput do artigo e, nesse caso mencionado, a ré foi condenada a sete anos, nove meses e dez dias de reclusão, ou seja, foi utilizado o aumento de pena presente no parágrafo quarto do artigo 171 do Código Penal para condenar a autora.

2.2.9 Pena e ação penal

Como já mencionado, as penas cominadas do delito de estelionato são reclusão de um a cinco anos, e multa. A pena pode ser majorada em hipóteses presentes no parágrafo terceiro e quarto e, pode ser diminuída nos casos de estelionato privilegiado.

A ação penal, a partir do acréscimo feito pelo §5º da Lei n. 13.964/2019 passou a ser como regra pública condicionada a representação, salvo se a vítima for a Administração Pública (direta ou indireta); criança ou adolescente; pessoa com deficiência mental ou; maior de 70 (setenta) anos de idade ou incapaz. Nessas hipóteses mencionadas a ação penal será pública incondicionada (Bittencourt, 2023, p. 173).

2.2.10 Concurso de crimes

O doutrinador Fernando Capez relata em sua doutrina que, é um caso bastante discutido na doutrina e jurisprudência a prática do delito de estelionato mediante o uso de documento falso, presente no artigo 307 do Código Penal Brasileiro. Neste caso o sujeito passivo seria o Estado portanto, atinge interesse público a prática desse delito, por sua vez, o estelionato atinge interesse particular da vítima. A questão é que há quatro posições presentes na doutrina e na jurisprudência em casos que o agente falsificar um documento público ou particular e com isso induzir alguém em erro para obter vantagem ilícita patrimonial diante disso (Capez, 2024)

A primeira posição, do Superior Tribunal de Justiça, menciona que o estelionato absorve a falsidade, quando esta foi o meio fraudulento empregado a

prática do crime-fim, que era estelionato. Diante disso, ressalva a Súmula 17 cujo teor é "*quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absolvido".* Já a segunda corrente relatada pelo Supremo Tribunal Federal diz que há concurso formal de crimes pelo fato de que os crimes mencionados atingem bens jurídicos diversos e, menciona que o crime de falsidade de documento público é mais severamente apenado que o crime de estelionato, assim argumentando sobre o afastamento da absorção de crimes. Existe um terceiro posicionamento na doutrina que diz que neste caso citado há concurso material. Por fim, o quarto posicionamento relata que o crime de uso de identidade falsa prevalece sobre o de estelionato, uma vez que a falsidade deve ser de documento público.

Por haver essa discussão na doutrina sobre a aplicação do concurso de crimes, não há uma corrente que seja majoritária neste caso, porém a doutrina tende a pender para o posicionamento relatado pelo Superior Tribunal de Justiça.

3 FRAUDE ELETRÔNICA

A fraude eletrônica, ou também chamada de estelionato virtual, está descrita nos parágrafos 2º-A e 2º-B do artigo 171 do Código Penal. O primeiro menciona casos em que a fraude é cometida com utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico ou algum outro meio análogo, e a pena para determinado fato típico é de 4 (quatro) a 8 (oito) anos de reclusão e, multa. Já o segundo, relata a respeito de hipótese em que o crime fora praticado mediante utilização de servidor mantido fora do território nacional, com aumento de pena de 1/3 (um terço) a 2/3 (dois terços), essa elevação ocorre pelo fato de que a origem dos ataques é hospedada no exterior, dificultando muito mais a investigação e a descoberta de autoria do delito (Nucci, 2024, p. 425).

Esta previsão, incluída pela Lei 14.155/2021, veio de encontro ao incremento das fraudes cometidas por diversos meios eletrônicos e informáticos, gerando novos e variados mecanismos capazes de armar ciladas para ludibriar as pessoas, cada vez mais levadas a esse cenário pelas inovações tecnológicas. É preciso lembrar que as transações bancárias têm sido promovidas pela internet e outros meios de comunicação, sem a presença do cliente na agência. Vários negócios são celebrados exclusivamente por meio eletrônico e isso fez com que os estelionatários migrassem para novas modalidades de fraude (Nucci, 2024, p. 425).

Diante deste cenário, pode se concluir que no cotidiano atual com o avanço da tecnologia, os infratores ou estelionatários, utilizam da má-fé para praticar o delito de estelionato contra pessoas de boa-fé que são enganadas por estes infratores.

3.1 Do direito digital

Sob perspectiva da globalização, a tecnologia se modernizou de modo abrangente e transformou profundamente a maneira como vivemos, interagimos e trabalhamos. Pode se dizer que a sociedade atual vem passando por uma espécie de Revolução Informática, que vem possibilitando a substituição do trabalho humano por máquinas (Crespo, 2011, p.12).

Com esse avanço, ressaltasse que grande parte da população global tem acesso à tecnologia em diversas áreas. Na área informativa, existem sites, blogs e jornais onde são divulgadas as informações que acontecem regularmente no dia a dia da população. Na área da indústria que pode ser notado pelo surgimento de máquinas modernas, que facilitam ou substituem algum tipo de trabalho braçal. Pode ser mencionado também os teletrabalhos, mais conhecido como *“homeoffice”,* que consiste no trabalho a distância, ou seja, o trabalhador não precisa se deslocar da sua casa até o ambiente de trabalho para que consiga concluir o seu expediente. Tais modernizações facilitaram grandemente as principais áreas de atuação do ser humano e possibilitou explorar caminhos jamais vistos.

Atualmente, com o surgimento da *blockchain* e a inteligência artificial, novos ambientes digitais podem ser desbravados e com isso, novas implicações vem à tona e com isso surge a necessidade de um campo jurídico especializado para que possa acompanhar e regular essas mudanças.

O conceito de direito digital é muito amplo e pode ser aplicado em diversas atividades que ocorrem no mundo virtual, como divulgação de conhecimento ou também de operações de compra e venda através de internet ou algum outro meio de comunicação.

Para a autora Patrícia Peck Pinheiro, a ideia do conceito de direito digital é a seguinte:

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicadas até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc (Pinheiro, 2021, p.71).

Com o avanço da internet, o campo do ciberespaço se tornou cada vez mais presente que nada mais é do que um espaço de comunicação por meio de rede de computação. Diante disso, o Ministério da Ciência e Tecnologia, pretendia garantir o desenvolvimento do país, com a inserção do programa da Sociedade da Informação, como diz Fiorrilo e Conte:

> O Brasil, por meio do Ministério da Ciência e Tecnologia, estabeleceu, no ano de 1997, um Programa para a Sociedade da Informação, que resultou na edição do Livro Verde da Sociedade da Informação, por meio do qual foram indicadas diversas metas com o fito de inserir o Brasil no contexto da

> Sociedade da Informação, bem como, dessa forma, garantir o desenvolvimento do País. (Fiorillo; Conte, 2016, p.19).

Diante de um campo tão abrangente como o do ciberespaço, decorreu da necessidade da criação de regras para que regulassem esse âmbito de modo que pudesse garantir os deveres e direitos de seus usuários, tendo um uso saudável desse campo. Em face do exposto, foram criadas duas leis federais que regulam as condutas ilícitas que são cometidas com a utilização de meios informáticos e outros dispositivos.

A Lei Federal nº 12.735 de 30 de novembro de 2012 promoveu mudanças no Código Penal, até mesmo no Código Penal Militar. A norma versa sobre condutas realizadas mediante o uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados. A norma dispões também a respeito dos órgãos da Polícia Judiciária que estruturarão setores e equipes especializadas no combate as ações praticadas por esses infratores contra rede de computadores, dispositivo de comunicação ou sistema informatizado (Migalhas, 2013).

> Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Por sua vez, a Lei Federal nº 12.737/2012 criminaliza a invasão de computadores, como o “roubo” das senhas e arquivos. A pena prevista no artigo é de 3 meses a 1 ano para quem invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagens ilícitas. Vale ressaltar que essa lei veio para acrescentar o disposto no artigo 154 do Código Penal, como está descrito no texto legal:

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e

> com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Diante do exposto, essas normas federais entraram em vigor com o intuito de diminuir ou até mesmo erradicar esse tipo de crime, representando um avanço significativo do Poder Judiciário brasileiro em relação ao combate de crimes cibernéticos no país e, assim, protegendo o patrimônio do cidadão de bem.

3.2 Marco Civil

O marco civil da internet, que foi introduzido pela Lei nº 12.965 de 23 de abril de 2014, representa um marco extremamente importante na regulamentação da utilização da internet no Brasil. Nesse cenário, foram introduzidos princípios, direitos e garantias para os usuários. Com o cenário atual do país em relação as fraudes eletrônicas, essa lei se torna ainda mais considerável, assegurando a privacidade e a proteção de dados dos usuários.

O termo “internet” foi adotado para significar todo o conjunto de tecnologias de informação e comunicação utilizadas pelos cidadãos brasileiros em suas interações virtuais e sociais (Gonçalves, 2017, p. 02).

O doutrinador Victor Hugo Pereira Gonçalves conceitua, em seu livro (Gonçalves, 2017, p.02), a internet como:

> Internet é um nome localizado no espaço e tempo restritos que pode, dentro em breve, ser ultrapassado por outras nomenclaturas melhores e mais atualizadas. Já há em curso uma revolução de convergências de mídias de comunicação, o que coloca em dúvida a utilização do conceito de internet, que foi formulado na década de 1990.

Essa lei é considerada a principal norma federal que regulamenta o uso da internet no Brasil, onde estão especificados os princípios fundamentais que regulam o marco e serão destrinchados nos próximos parágrafos.

3.2.1 Princípio da liberdade de expressão e democracia

Para introduzir este princípio de forma mais detalhada, é necessário abordar um contexto histórico do pensamento político e jurídico, que teve seu ápice nos Estados Unidos da América.

Nos Estados Unidos, pode se dizer que o momento de afirmação da liberdade de expressão do pensamento dentre as garantias asseguradas pela Constituição do país com a edição da Primeira Emenda (*First Amendment*), que foi promulgada em 1791 como parte da Carta de Direitos (*Bill of Rights*) e uma de suas proteções era a proibição de qualquer lei que limitasse a liberdade de expressão (Leite, Lemos, 2014, p. 128).

A *First Amendment* tinha o intuito de impedir que o governo federal, estadual e locais criassem leis que restringissem ou censurassem o direito da livre expressão dos cidadãos.

A liberdade de expressão, do termo em inglês "*freedom of speech"* não está relacionada apenas a forma de se manifestar verbalmente. A palavra "*speech"* vai além e abrange também formas de pensamento, manifestações artísticas, protestos, entre outros. Então, significa que a liberdade de expressão protege qualquer discurso proferido pelos cidadãos seja ele político, cultural ou religioso.

Contudo, mesmo com o texto amplo e abrangente mencionado na Primeira Emenda, a liberdade de expressão não era algo absoluto. Assim como em vários outros países, a Suprema Corte Americana estipula limites para esses princípios e repudia condutas de violência, difamação ou ameaças proferidas por qualquer cidadão.

Já no Brasil, o texto constitucional de 1988 traz a liberdade de expressão como um conjunto de liberdades, chamados de garantias fundamentais, como pode ser previsto no artigo 5º e seus incisos da Constituição Federal:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
> V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
> VI - é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias;

> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XIII - é livre o exercício de qualquer trabalho, ofício ou profissão, atendidas as qualificações profissionais que a lei estabelecer;
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional.

Como pode ser notado, a *freedom of speech* proveniente da Primeira Emenda dos Estados Unidos, influenciou diretamente para a formação da liberdade de expressão que temos hoje no Brasil e abarca diversas espécies como a liberdade de manifestação do pensamento, de consciência e expressão religiosa, da atividade intelectual, artística, cientifica, da comunicação e informação (Leite, Lemos, 2014, p. 130).

No contexto do Marco Civil, a liberdade de expressão é um direito fundamental que deve ser protegido. o artigo 3º da lei nº 12.965/2014 menciona que a utilização da internet no país deve seguir os termos da Constituição Federal.

No entanto, é de suma importância mencionar que também no Brasil, o direito à liberdade de expressão é algo relativo. Esse direito deve ser utilizado de maneira responsável e respeitando qualquer outro direito, como por exemplo o da privacidade. O Marco Civil estabelece um equilíbrio a respeito da liberdade de expressão e a responsabilidade civil, onde cidadãos que utilizarem essa liberdade para violar direitos de terceiros serão responsabilizados civilmente.

3.2.2 Princípio da neutralidade da rede

O princípio da neutralidade da rede estabelece que os provedores de internet forneçam um uso igualitário para os usuários em geral, sem bloquear sites ou dificultar o acesso destes. Outro ponto deste princípio é que ele impede que os provedores cobrem preços diferentes para o acesso de diferentes sites, ou seja, os usuários não devem pagar preços alternativos dependendo do site que utilizarem. O que é permitido para os provedores é cobrar tarifas diferentes a respeito da quantidade de velocidade fornecida para o usuário.

Os doutrinadores Ronaldo Lemos e George Salomão Leite, mencionam que este princípio visa impedir três tipos de discriminação, sendo elas o bloqueio, a discriminação pela velocidade e por preço.

Resumidamente, o bloqueio seria a restrição completa dos usuários a determinados sites. A discriminação por velocidade se divide em duas: positiva e negativa. A primeira está relacionada ao aumento de velocidade do acesso de terminadas aplicações e a segunda sobre a redução dessa mesma velocidade. Já a discriminação por preço também foi dividida em positiva e negativa e, também, segue a mesma lógica. A positiva visa a redução das tarifas, enquanto a negativa o aumento destas.

3.2.3 Princípio da garantia da privacidade de dados pessoais

Esse princípio reflete diretamente no cenário atual, pelo fato de que cada indivíduo deve ter o direito de ter suas informações pessoais respeitadas e protegidas. Essa garantia se tornou essencial com o avanço gradativo da tecnologia para a preservação da autonomia e a dignidade do cidadão. Tal princípio não somente protege dados contra outros acessos, mas também garante a segurança dos usuários em relação ao controle sobre as informações que são utilizadas e compartilhadas, como é o caso das senhas que são salvas nos navegadores e, diante disso, promove a confiança nas relações praticadas no meio digital.

Acerca da privacidade, a Constituição Federal de 1998, menciona em seu artigo 5º, um amplo rol de direitos e garantias fundamentais dos cidadãos, inclusive a proteção à intimidade, privacidade e aos dados (elencado nos incisos X e XII). Tais previsões são mencionadas também no Código Civil em seu artigo 21 (Leite, Lemos, 2014. p.152):

> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Diante da importância do assunto, a privacidade e proteção dos dados pessoais foram tratados como princípios fundamentais que foram estabelecidos mais especificamente no artigo 3º, incisos II e III e artigo 7º, incisos VIII e IX:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

É importante frisar que o Marco Civil abrangeu diversas áreas do direito até mesmo a relação de trabalho entre o empregado e o empregador, onde a partir desse princípio foi possível aperfeiçoar o monitoramento das atividades *onlines* praticadas pelos empregados em horário de expediente, como destaca os doutrinadores George Salomão Leite e Ronaldo Lemos:

> É fundamental observar, então se os empregadores podem monitorar as atividades de seus empregados, quando da utilização da infraestrutura tecnológica corporativa, abrangendo o uso de dispositivos informáticos, da internet e de aplicações eletrônicas, em geral, tais como e-mail, navegação, entre outros (Leite, Lemos, 2014, p. 153).

Portanto, este princípio é uma diretriz fundamental na proteção dos dados pessoais que se encontram no meio digital, buscando a segurança deles garantindo a segurança e seus devidos direitos. Vale ressaltar que este princípio estabelece que os dados que forem armazenados devem ser coletados de forma limpa e segura e assim, garantindo a proteção das informações de cada usuário.

O que é importante mencionar é que dentre os princípios mencionados, todos eles visam o melhor funcionamento do meio digital, buscando a segurança e privacidade dos seus usuários. Porém, mesmo com tantos pontos positivos, existem a pessoas de má índole que utilizam destes meios para se beneficiar de forma ilícita de terceiros que acabam sendo coagidos ou enganados.

3.3 Variedades de modalidades de estelionato virtual e casos concretos

O estelionato praticado mediante o uso do meio digital cresceu gradativamente no Brasil desde 2018. Naquele ano 426.799 golpes foram registrados, enquanto no ano de 2022 o número quadriplicou, totalizando 1.819.409 casos em registro (G1, 2023). Tal cenário mostra que os criminosos, a cada ano que passa,

aperfeiçoam cada vez mais seus métodos para ludibriar cidadãos de bem e assim obter alguma vantagem ilícita sobre eles. Iremos citar alguns tipos de golpes que vem sendo utilizados pelos infratores.

3.3.1 *Pishing*

Com a imensidade de golpes praticados pelos criminosos, um dos mais utilizados é conhecido como “*phishing*”. Tal conduta é conceituada como um ataque cibernético que consiste no envio de e-mails, mensagens de texto, telefonemas ou sites fraudulentos para enganar as pessoas a compartilhar dados pessoais e confidenciais.

O termo “*pishing”* é derivado da palavra em inglês “*fishing*” que significa “pescaria”. O golpe consiste em criar iscas virtuais, para que usuários desavisados acabem “caindo” nelas.

No momento em que a vítima adentra nesses sites fraudulentos, é solicitado a ela diversas informações pessoais como e-mail, número do RG ou CPF, número de telefone, entre outros. As informações obtidas por esses criminosos são utilizadas posteriormente para aplicar golpes em outros usuários.

Portanto, os ataques de *phishing* são a prática de enviar notificações fraudulentas que parecerem estar sendo enviadas de fontes confiáveis, cujo objetivo é descobrir dados confidenciais como senhas de cartão de crédito ou informações de login, entre outros (SERASA, 2024).

Um exemplo prático desse delito são e-mails de empresas com grande renome, como é o caso dos Correios. Os criminosos criam um site com uma interface bem parecida com ao site verdadeiro e encaminham *links* para os usuários com mensagens que chamam a atenção de quem está lendo, como por exemplo dizendo que a encomenda que a pessoa comprou está retida pela fiscalização alfandegária e para que esta seja liberada, deve ser pago uma quantia monetária. Gozando da ingenuidade das pessoas, os infratores conseguem obter esses valores facilmente pois os cidadãos acabam ficando receosos de serem taxados ou que vão “sujar” o seu nome.

Outro exemplo que pode ser mencionado são os e-mails de instituições bancárias. Os infratores encaminham uma mensagem eletrônica idêntica a aquelas encaminhadas por bancos e na mensagem consta a seguinte frase “urgente, atualize

suas informações de conta". No corpo do texto do e-mail diz que foi detectada uma atividade suspeita em sua conta e que as informações pessoais precisam ser alteradas. Para isso eles encaminham um link ou alguma opção que leve a vítima a esse link e nele pede para inserir os dados bancários e essa acaba inserido por ser idêntico ao do respectivo banco. E diante disso, os criminosos possuem acesso as instituições bancárias dessas pessoas e subtraem o dinheiro delas ou fazem empréstimo em seus nomes.

3.3.2 *Catfishing*

Catfishing é um termo utilizado para caracterizar o infrator que utiliza de imagens e informações falsas para criar uma identidade falsa no mundo digital para assim enganar e fraudar algo de outra pessoa (CNN BRASIL, 2024).

Na maioria dos casos que são registrados, os criminosos se utilizam de um perfil falso em sites de relacionamentos e criam um vínculo afetivo e sentimental com a vítima.

O "*catfisher*", termo utilizado para denominar o infrator, desenvolve uma identidade que acha que atrairá seu alvo, falsificando certos aspectos de seu perfil, como por exemplo escolher uma foto de perfil mais atraente (FORTINET, 2024). Nesses casos, os golpistas não aceitam realizar chamadas por vídeo ou se encontrar presencialmente com a pessoa que está criando vínculo.

Uma dúvida que está presente na doutrina a respeito do caso é se existe responsabilidade jurídica dos aplicativos de relacionamento e, diante disso, Rodrigo da Cunha Pereira leciona:

> Os aplicativos, sites e similares de relacionamentos não são responsáveis pelos encontros e desencontros de relações extraconjugais. Os encontros que ali acontecem se dão entre pessoas adultas e são elas mesmas as responsáveis pelos encontros, por mais que o encontro tenha trazido prejuízos, dores de amor, ciúmes, etc. Encontros malsucedidos podem acontecer vi cal ou presencialmente, ainda que seja apenas para encontros sexuais. E não existe sexo ilegítimo. Reações sexuais ilegítimas são apenas aquelas não consentidas ou entre pessoas incapazes (Pereira, 2023)

Um caso que ficou mundialmente conhecido foi o do "Golpista do Tinder", que foi detalhado em um documentário exibido pela empresa de *stream*, Netflix. No enredo, Simon Leviev (golpista) enganava mulheres que encontrava no aplicativo de

relacionamento Tinder. Simon se passava por um milionário nas redes sociais e solicitava empréstimos para essas mulheres mediante a falsas promessas. Os prejuízos foram significativos e gira em torno de US$10 milhões (cerca de R$52 milhões de reais).

No Código Penal Brasileiro ainda não existe uma norma vigente que prevê o "*catsishing"* como crime, porém existe um projeto de lei que tramita na Câmara dos Deputados para que tal delito seja incluído. O objetivo desse projeto é incluir no artigo 171 do Código Penal o crime de estelionato sentimental cuja descrição é quando o infrator "induz a vítima, com promessa de constituição de relação afetiva, a entregar bens ou valores para si ou para outrem".

3.3.3 Golpe do boleto falso

Os golpes praticados mediante boletos falsos é uma modalidade de estelionato que vem se tornando cada vez mais frequente no âmbito digital. Ocorre quando os golpistas encaminham boletos fraudulentos por meios digitais. No boleto constam informações verídicas como nome e CPF e assim, induzindo o pagamento sem perceber que o dinheiro está indo para a conta de outro destinatário, neste caso, o golpista (BRADESCO, 2024).

Um exemplo prático que pode ser mencionado é o caso dos falsos boletos de conta de água. Os criminosos encaminhavam um boleto idêntico ao das empresas responsáveis pelo serviço e os moradores efetuavam o pagamento achando que estavam pagando de forma correta. Os criminosos deixavam o boleto muito parecidos, com informações verídicas como endereços, nome do proprietário do imóvel, CPF. A única coisa que era diferente seria o destino do pagamento que seria a conta de criminosos.

Uma alternativa dos criminosos é emitir uma segunda via do boleto e encaminhar para os cidadãos alegando que a primeira via do boleto não havia sido paga. A prefeitura da cidade de Boituva/SP, público uma nota em seu site oficial alertando a população desse golpe que estava acontecendo na cidade:

> A Sabesp pede atenção dos clientes sobre um golpe que está sendo aplicado por um site falso para emissão de segunda via de contas e pagamento através do PIX: Trata-se de golpes e as medidas cabíveis serão tomadas pela Empresa (BOITUVA, 2024).

A própria empresa Sabesp, em um perfil de sua rede social alertou os moradores sobre este suposto golpe:

> A Sabesp pede atenção dos clientes sobre um golpe que está sendo aplicado por um site falso para emissão de segunda via de contas e pagamento através do PIX: Trata-se de golpes e as medidas cabíveis serão tomadas pela Empresa (SABESP, 2024).

Diante deste cenário, é necessário a atenção dos moradores na verificação do destinatário para o pagamento, para que assim evite ser vítima do golpe do boleto falso.

3.3.4 Golpes em lojas virtuais

As famosas lojas virtuais, ou também conhecidas como e-commerce, trouxeram uma maior facilidade para os compradores, possibilitando a compra e venda de mercadoria via internet.

No entanto, a partir deste cenário, criminosos se aproveitaram para praticar o crime de estelionato utilizando o e-commerce. Aproveitando o aumento das compras online, os golpistas criam lojas falsas ou simplesmente clonam os sites de empresas que já existem e atraem as vítimas com ofertas irrecusáveis. Na maioria dos casos os produtos comprados sequer chegam aos seus destinatários ou quando chegam, estão totalmente defeituosos.

Dentro deste tópico pode ser citado diversos métodos utilizados pelos criminosos para convencer o comprador a adquirir o produto e assim, obter a consumação do delito de estelionato. Um método muito praticado pelos criminosos é o golpe da OLX, na compra e venda de carros, chamado de golpe da venda intermediada. O portal da Polícia Civil do estado do Paraná publicou um passo-a-passo de como os golpistas realizam esse golpe:

> O golpista copia um anúncio de venda e cria outro anúncio com seu número de contato. O comprador vê o anúncio e entra em contato com o golpista que faz uma intermediação da venda, simulando o pagamento de uma dívida com um primo ou algum parente e pede para que comprador e vendedor originário se vejam, mas não negociem valores entre eles. O comprador fecha negócio com o golpista e faz o pagamento na conta indicada por ele. Quando se encontram em cartório para fazer a transferência do veículo, comprador e vendedor tomam ciência de que caíram em um golpe (PARANÁ, 2024).

Outro método utilizado pelos infratores são os golpes em que eles se deparam com o anúncio do vendedor em um site de compra e venda, onde constam suas informações, como é o caso do número vinculado ao *WhatsApp* do vendedor.

Logo em seguida, o golpista manda uma mensagem via *WhatsApp* solicitando um código de confirmação que fora enviado via SMS para o vendedor. O infrator menciona que o código é apenas para verificação ou outro motivo semelhante, porém é o código de acesso ao aplicativo de mensagem do anunciante e assim acaba o enganando e clonando o seu *WhatsApp*. Diante disse, o infrator aplica golpes nas pessoas se passando por pelo anunciante e essas acabam mandando o dinheiro. O site de informações Tecnoblog, mencionou um caso em que um usuário teve seu aplicativo clonado:

> Marcos Lopes publicou um anúncio na OLX para vender um relógio. Ele recebeu uma mensagem via WhatsApp pedindo um código de confirmação; o contato tinha o logotipo da OLX na imagem de perfil, então ele enviou. Em pouco tempo, cerca de 300 pessoas receberam mensagens da conta dele pedindo dinheiro emprestado; um amigo acabou transferindo R$ 500 (TECNOBLOG, 2024).

É essencial a atenção dos usuários para supostas mensagens solicitando informações pessoais ou supostos códigos de verificação para que assim não se tornem vulneráveis aos estelionatos virtuais. E vale ressaltar, a importância de as pessoas desconfiarem caso alguma outra pessoa entre em contato solicitando alguma transferência, evitando um suposto golpe.

3.3.5 Golpe do falso leilão

Esse golpe é muito conhecido no mundo digital e que é muito aplicada por criminosos. Criminosos criam sites de leilões falsos, com a aparência idêntica ao site verdadeiro.

Eles pagam para que sejam entregues para as pessoas por forma de anúncio onde o produto está muito abaixo do valor médio das arrematações dos leilões verdadeiros. O Ministério Público do Estado de Minas Gerais público um documento explicando detalhadamente como os criminosos agem a partir do

momento em que conseguem enganar a vítima fazendo com que ela clique no anúncio:

> Depois que a vítima se cadastra e envia sua oferta, os criminosos entram em contato solicitando cópias de documentos pessoais e o depósito do valor do lance. Após receberem o pagamento e as cópias dos documentos, encerram o contato com a vítima e usam os seus dados para aplicarem novos golpes em terceiros (MINAS GERAIS, 2024).

Um caso que pode ser mencionado é o de uma quadrilha de Minas Gerais que foi presa após aplicar diversos golpes na população em geral. De acordo com as investigações, o grupo agia em diversos estados do Brasil e teria movimentado um milhão de reais em apenas um único mês (CNN BRASIL, 2024).

Outro caso que pode ser mencionado aconteceu no estado de Santa Catarina, onde outra quadrilha foi detida por aplicarem o golpe do falso leilão. O Tribunal de Justiça do estado, relata que dentre os meses de janeiro de 2022 e agosto de 2023 o grupo de estelionatários deu um total de R$ 18 milhões de reais em prejuízo para as vítimas, apenas em Santa Catarina (TJSC, 2024).

Na maioria dos casos, os criminosos criam um site falso de leilões do governo, como por exemplo o leilão da Receita Federa, ou outros órgãos públicos. O Tribunal de Justiça do Estado de São Paulo discorreu sobre esses acontecimentos:

> Quadrilhas especializadas em golpes costumam utilizar o nome, logotipo e/ou informações de empresas, escritórios de advocacia, bancos e instituições públicas, como o Tribunal de Justiça de São Paulo, para ludibriar o cidadão e praticar crimes diversos, seja através de telefonemas, mensagens por aplicativo, cartas ou mesmo com a criação de falsos sites de leilões (TJSP, 2024).

Diante desse cenário, as pessoas acreditam que os sites são verdadeiros e que os leilões estão sendo promovidos por órgãos do governo ou semelhantes. Nesse contexto, essas pessoas acabam sendo vítimas desses criminosos e tem seu dinheiro subtraído.

3.4 Métodos de Prevenção contra o crime de estelionato virtual

Com a crescente prática do delito por parte dos criminosos, o alerta para a população deve ser fundamental e este pode ser feito de diversas formas, como em propagandas publicadas em meios de comunicação ou campanhas de conscientização proporcionadas pelos entes públicos, pelo fato de que com o aumento

das transações realizadas de modo digital, fez com que os criminosos utilizassem métodos cada vez mais sofisticados.

A seguir, será mencionado algumas medidas que podem ajudar a prevenir a população em geral de se configurar como vítima do delito de estelionato no “mundo virtual”.

Primeiramente, a suposta vítima do estelionatário deve se atentar ao remetente que encaminhou o e-mail ou que entrou em contato em seu celular. A maioria dos criminosos encaminham e-mails similares aos de grandes empresas, com a mesma logotipo e interface e isso acaba gerando uma confiança na vítima. Porém, em grande parte dos casos, o endereço de e-mail do remetente nem sempre tem o nome da empresa ou quando tem, está acompanhada de diversos números e caracteres diversos, como símbolos. Normalmente, os criminosos trocam uma única letra do e-mail, fazendo com que até mesmo aqueles que estão atentos com o golpe, acabem sendo vítimas. Outra medida cabível, é a utilização do padrão DMARC (*Domain-based Message Authentication Reporting and Conformance*) que é um método de autenticação de mensagens recebidas no e-mail, ou seja, se essa mensagem eletrônica for reprovada pelo padrão DMARC, ela vai ser direcionada para o spam ou lixo eletrônico (CLOUDFLARE, 2024). Portanto, os usuários devem sempre desconfiar das mensagens que recebem em sua caixa de entrada e analisar o remetente, assim se prevenindo de golpes de *phishing*.

A respeito dos golpes praticados mediante boleto falso, uma medida viável para se prevenir é sempre conferir se os dados do beneficiário correspondem ao de quem vendeu o produto ou serviço. Outra medida cabível é sempre desconfiar, caso o código de barras presente falhas ou esteja com um espaço excessivo ou qualquer outra alteração que impeça o reconhecimento pelo leitor (POLÍCIA CIVIL, 2024). Deve ser observado o valor presente no boleto, como menciona o portal do Serasa:

> “O valor do boleto aparece em dois lugares, no final do código de barras e no espaço “valor do documento”. Caso o valor não seja igual, desconfie que você está com boleto falso. Outro sinal de alerta, é constar um preço diferente em uma cobrança que costuma ter um valor fixo (SERASA, 2024).”

Porém se estiver sendo vítima do crime de estelionato sentimental, existem alguns meios para se proteger. Especialistas mencionam que as vítimas não podem ter medos de fazer perguntas diretas ou desafiar a pessoa que suspeita estar

enganando-a, como por exemplo o motivo dela não querer fazer chamadas por vídeo ou se encontrar presencialmente (CNN BRASIL, 2024). A solução é interromper as comunicações com o golpista e evitar mandar dinheiro a eles.

Ademais, para se prevenir de estelionatários que utilizam lojas virtuais para concretizar seus golpes existem diversos caminhos. Um deles é sempre fazer negócios com clientes que possuem o selo de verificação da loja de *e-commerce* que você está utilizando, pois se aquele perfil foi verificado, presume-se que está apto para realizar compra e venda dentro do site. Outra medida, é evitar compartilhar dados pessoais para outros usuários, como o número de telefone, exemplo. A empresa de compra e venda de mercadorias, Mercado Livre, lecionou a respeito:

> Para garantir uma negociação segura, o Mercado Livre orienta seus clientes a sempre realizarem os contatos logados à plataforma. A empresa destaca que, precisamente para garantir a segurança dos usuários, dados de contato como endereço de e-mail e número de celular não devem ser informados a outros usuários diretamente antes da concretização da venda/compra do produto por meio da plataforma. Também orienta que esses dados não sejam trocados por e-mail ou mensagens (MERCADO LIVRE, 2024).

A empresa OLX, também se pronunciou a respeito de como se prevenir dos golpistas que estão presentes no aplicativo (OLX, 2024):

> Para que nossos usuários possam realizar negociações on-line bem-sucedidas entre eles, a OLX investe continuamente em tecnologia e na comunicação de melhores práticas de compra e venda, informando-os inclusive sobre como proceder em casos de tentativas de fraudes, com alertas em nossos canais oficiais e redes sociais. A OLX reforça que não solicita código de verificação ou senhas para nenhum usuário e recomenda que as negociações aconteçam via chat, na plataforma (OLX, 2024).

Se os criminosos tentarem invadir o seu aplicativo do *Whatsapp* ou outro aplicativo para que assim realizem outros delitos de estelionato, a medida cabível é autorizar a função de “autenticação dois fatores”, que consiste no envio de um código via SMS ou por telefone em que autorize a entrada no respectivo aplicativo. Cabe ressaltar que este código jamais deve ser compartilhado ou encaminhado para outra pessoa e que as lojas virtuais jamais solicitam esses códigos de verificação e isso nada mais é do que mais uma maneira que os criminosos utilizam para adentrar em seu aplicativo se passando por empresas.

Por fim, para se prevenir do golpe do falso leilão, é necessário também sempre verificar o nome da conta que está recebendo o pagamento. Como

mencionado anteriormente, na maioria dos casos, os criminosos criam leilões parecidos com os que os entes públicos realizam, ou seja, leilões judiciais. O Tribunal de Justiça do Distrito Federal leciona a respeito do caso:

> Em caso de opção pela compra, como regra nos leilões judiciais do TJDFT, o pagamento deve ser realizado mediante guia de depósito judicial vinculada ao respectivo processo judicial, ou Guia de Recolhimento da União, no caso de leilões administrativos. Nunca realize pagamento para contas de pessoas físicas (TJDF, 2024)

Deve ser analisado se existem erros de português nas publicações feitas dentro do site falso, pois é muito comum que isso ocorra. E, por fim, sempre desconfiar caso o preço do bem leiloado esteja com um preço de arrematação muito abaixo do normal, pelo fato dos criminosos utilizarem essas condutas para atraírem suas vítimas (TJRS, 2024).

3.5 Estelionato virtual e o direito comparado

Internacionalmente, o crescimento da dependência dos aparelhos eletrônicos tem facilitado o crescimento das fraudes praticadas pelo meio digital, assumindo diversas modalidades ao redor do mundo. A utilização da inteligência artificial (IA), modelos de linguagem e criptomoedas combinados com modelos de *phishing* resultam em golpes mais sofisticados e sem a necessidade de um custo alto para ser realizado (INTERPOL, 2024).

A própria Interpol menciona que as modalidades de golpes mais recorrentes são os golpes de investimentos, sentimental, pagamento antecipado e aqueles praticados via *e-mail*. (INTERPOL, 2024).

Foi criado um mecanismo chamado *Global Rapid Intervation of Payments (I-GRIP),* que consiste na rápida intervenção em golpes financeiros. Esse mecanismo tem uma colaboração intensa da Interpol, instituições financeiras e entes do poder judiciário. Primeiramente o I-GRIP detecta quando alguma transação suspeita é realizada e assim inicia um protocolo de resposta rápida que envolve o contato com as instituições financeiras relevantes para bloquear a transação. Logo em seguida, a Interpol contato os órgãos judiciários para acompanhar esses fundos que foram bloqueados, para fins de novas evidências. Por fim, acontece a

recuperação do valor e a devolução aos donos originários (Swiss Security Solutions, 2024).

Na América do Norte, o FBI também age com alto desempenho na prevenção contra os golpes praticados no meio digital e em seu portal traz o seguinte posicionamento:

> A estratégia cibernética do FBI é impor riscos e consequências aos adversários cibernéticos. Nosso objetivo é mudar o comportamento de criminosos e estados-nação que acreditam que podem comprometer redes dos EUA, roubar propriedade financeira e intelectual e colocar infraestrutura crítica em risco sem enfrentar riscos eles próprios. Para fazer isso, usamos nossa combinação única de autoridades, capacidades e parcerias para impor consequências contra nossos adversários cibernéticos (FBI, 2024).

O FBI trabalha de modo que possa evitar que os possíveis golpes ocorram, e para isso eles possuem esquadrões cibernéticos altamente treinados em cada um dos 55 escritórios que possuem. Eles também possuem assistentes cibernéticos em todas as embaixadas americanas ao redor do mundo e com a colaboração do *Internet Crime Complaint Center (IC3)* que coleta dados das pessoas vítimas dos golpes digitais, bloquearam centenas de milhares de dólares e conseguiriam restituir os valores para as vítimas. Vale ressaltar que o FBI também possui o *CyWatch* que é um centro de operações 24 horas que fornece suporte para as vítimas (Federal Bureau of Investigation, 2024).

No continente europeu, o principal órgão responsável pelo combate das fraudes eletrônicas é a Europol que atua diretamente nos países que fazem parte da União Europeia. Por meio de relatórios chamados de *Spotlight Report* que abordam os golpes em geral e analisa cada um deles para que assim possam ter um controle a respeito do delito (Europol, 2023).

Já no continente asiático, as fraudes onlines vêm se intensificando com o mundo digital. De acordo com o UNODC (Escritório das Nações Unidas sobre Droga e Crimes) foi estimado perdas financeiras de até 37 bilhões de dólares decorrentes de práticas golpistas apenas no ano de 2023 (UNODC, 2024). Cabe mencionar os golpes realizados mediante cassinos online, cenário que dominou a internet em esfera global, mas se intensificou ainda mais no continente asiático, cenário que acaba dificultando os órgãos estatais a combater esses grupos de golpistas.

Por fim, no continente africano, os golpes praticados via internet também estão muito presentes e de acordo com dados do provedor VPN Surfshark a África do

Sul é o quinto país com maior densidade em relação os golpes onlines, dados que *South African Banking Risk Information Centre (SABRIC)* também confirma. A principal modalidade praticada pelos criminosos é o *phishing* e com o surgimento da Inteligência Artificial, novos golpes vêm sendo atreladas a ela. Diante deste cenário, as instituições estatais e financeiras do continente africano estão cada vez mais fortalecendo sua segurança para proteger os usuários das fraudes online (ThreatMark, 2024).

4 CONCLUSÃO

O estudo do crime de estelionato e sua evolução histórica revela o quão complexo é esse delito e a sua adaptação ao decorrer dos anos. Historicamente o estelionato evoluiu de prática mais arcaicas de fraude para práticas mais sofisticadas envolvendo grandes operações enganosas no cotidiano atual. O delito esteve presente desde a antiguidade, como por exemplo na Grécia Antiga, até o contexto contemporâneo onde o uso dos meios digitais influenciou aos infratores para que concretizem o crime.

No texto legal brasileiro, o estelionato está elencado no artigo 171 do Código Penal, onde define e descreve suas modalidades. Houve diversas adaptações ao longo dos anos para abarcar as diferentes formas de estelionato, desde as fraudes comuns até as fraudes que envolvem algum meio tecnológico avançado. O legislador se preocupou em enquadrar de maneira precisa as diversas situações em que o crime pode ocorrer, mencionando as classificações do crime, seja quanto ao objeto material, meio empregado, entre outras.

O Código Penal prevê penas distintas para as diferentes modalidades do crime de estelionato para proteção eficácia da lei penal e proteger o patrimônio da sociedade. A sociedade deve estar informada sobre as diversas modalidades de estelionato e os métodos de se proteger contra elas.

Contudo, deve ser levado em consideração que o crime de estelionato continua sendo um desafio significativo para o Direito Penal Brasileiro sendo necessário um entendimento profundo de suas diversas modalidades e um método eficaz para repeli-lo. A história do delito e as diversas formas para praticá-lo devem ser levadas em consideração para que a justiça e a segurança econômica da sociedade sejam resguardadas.

Ressalta que o estelionato virtual, vem se tornando um grande problema na era digital exigindo que os órgãos governamentais exerçam seu poder para repelir esses delitos. Explorando os princípios do Marco Civil da internet, foi mostrado a importância desse cenário para garantir os direitos e deveres de todo cidadão. As modalidades de estelionato virtual apresentadas enfatizam a necessidade do Estado de aprimorar as medidas de proteção contra esse delito.

Por fim, conclui-se a monografia comparando o crime de estelionato com as práticas internacionais, demonstrando que é essencial a cooperação dos países para o combate desse delito.

Nesse cenário, percebe-se que o estelionato digital está presente em todas as regiões do planeta, com diferentes métodos de ser realizado e sempre tendo inovação por parte dos criminosos para que o delito venha a se concretizar. Diante disso, infere-se a necessidade de os órgãos governamentais buscarem melhorias para que possam combater esses criminosos e, além disso, devem promover campanhas de conscientização entre a população para que possam ter ciência e identificar que estão sendo vítimas desse delito.

REFERÊNCIAS

BALDAN, Édson Luís. Estelionato. **Enciclopédia jurídica da PUC-SP**. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Penal. Christiano Jorge Santos (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/425/edicao-1/estelionato. Acesso em: 19 out. 2024.

BITENCOURT, Cezar R. **Tratado de direito penal: parte especial. Crimes contra o patrimônio até crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 155 a 212). v.3. pp. 158-175**. São Paulo: SRV Editora LTDA, 2023. E-book..

BITENCOURT, Cezar Roberto, **Tratado de Direito Penal**, São Paulo: Saraiva, 2012.

BOITUVA. **Sabesp: atenção ao emitir segunda via de contas e pagamentos via Pix**. Disponível em: https://www.boituva.sp.gov.br/imprensa/noticias/sabesp-atencao-ao-emitir-segunda-via-de-contas-e-pagamentos-via-pix#:~:text=A%20Sabesp%20pede%20aten%C3%A7%C3%A3o%20dos,cab%C3%ADveis%20ser%C3%A3o%20tomadas%20pela%20Empresa.&text=Fique%20atento%20e%20confira%20todos,pagamentos%20em%20nome%20de%20terceiros. Acesso em: 19 out. 2024.

BRADESCO. **Golpe do boleto falso**. Disponível em: https://banco.bradesco/seguranca/prevencao-de-golpes/golpe-boleto-falso.shtm. Acesso em: 19 out. 2024.

BRASIL. **Código Criminal do Império do Brasil**. Lei de 16 de dezembro de 1830. Planalto.gov.br. Disponível em: <https://planalto.gov.br/ccivil_03/leis/lim/lim-16-12-1830.htm>. Acesso em: 1 jun. 2024.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 02 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 14 out. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União: seção 1, Brasília, DF, 02 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 14 out. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 out. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 19 out. 2024.

CAPEZ, Fernando. **Curso de direito penal: parte especial: arts. 121 a 212. v.2.** São Paulo: SRV Editora LTDA, 2024. E-book. ISBN 9788553622672. Acesso em: 22 mai. 2024.

CLOUDFLARE. ***O que é um registro DMARC?*.** Disponível em: https://www.cloudflare.com/pt-br/learning/dns/dns-records/dns-dmarc-record/. Acesso em: 24 out. 2024.

CNN BRASIL. **O que é catfishing e o que você pode fazer se for vítima**. Disponível em: https://www.cnnbrasil.com.br/tecnologia/o-que-e-catfishing-e-o-que-voce-pode-fazer-se-for-vitima/. Acesso em: 16 out. 2024.

CNN BRASIL. **Polícia prende quadrilha que aplicava golpe do falso leilão**. CNN Brasil, 22 out. 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/policia-prende-quadrilha-que-aplicava-golpe-do-falso-leilao/. Acesso em: 22 out. 2024.

CRESPO, Marcelo Xavier de F. **Crimes digitais**. Rio de Janeiro: Grupo GEN, 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 09 set. 2024.

DAMÁSIO E. de Jesus, **Código Penal anotado, cit., p. 613**; Julio Fabbrini Mirabete, Manual, cit., v. 2, p. 303. Em sentido contrário, E. Magalhães Noronha, Direito penal, cit., v. 2, p. 372.

DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 19 out. 2024.

DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 19 out. 2024.

EUROPOL. **Spotlight Report on Online Fraud – IOCTA 2023**. Disponível em: https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023. Acesso em: 26 out. 2024.

FEDERAL BUREAU OF INVESTIGATION. **Cyber Crime**. Disponível em: https://www.fbi.gov/investigate/cyber. Acesso em: 26 out. 2024.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação**. 2ª. Ed. São Paulo: Saraiva, 2016

FORTINET. **O que é catfishing?** Disponível em: https://www.fortinet.com/br/resources/cyberglossary/catfishing. Acesso em: 16 out. 2024.

FRAUD.COM. **The History and Evolution of Fraud**. Disponível em: <https://www.fraud.com/post/the-history-and-evolution-of-fraud>. Acesso em: 19 out. 2024.

G1. **Estelionatos no Brasil mais que triplicam em cinco anos e golpes virtuais disparam após pandemia, revela Anuário**. São Paulo, 20 jul. 2023. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2023/07/20/estelionatos-no-brasil-mais-que-triplicam-em-cinco-anos-e-golpes-virtuais-disparam-apos-pandemia-revela-anuario.ghtml. Acesso em: 16 out. 2024.

GONÇALVES, Victor Eduardo R. Sinopses Jurídicas v 09 - **Direito penal:** dos crimes contra o patrimônio aos crimes contra a propriedade imaterial – verificado. São Paulo: SRV Editora LTDA, 2020. E-book. ISBN 9788553619962. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553619962/. Acesso em: 22 mai. 2024.

GONÇALVES, Victor Hugo P. **Marco Civil da Internet Comentado**. Rio de Janeiro: Grupo GEN, 2016. E-book. ISBN 9788597009514. Acesso em: 26 set. 2024.

GROENINGA, Giselle. PEREIRA, Rodrigo da Cunha. **Relações virtuais pelo olhar da Psicologia e do Direito**. Boletim AASP, 2023.

Há 190 anos, 1º Código Penal do Brasil fixou punições distintas para livres e escravos. Disponível em: <https://www12.senado.leg.br/noticias/especiais/arquivo-s/ha-190-anos-1o-codigo-penal-do-brasil-fixou-punicoes-distintas-para-livres-e-escravos>. Acesso em: 19 out. 2024.

HUNGRIA, Nélson, **Comentários, cit., v. VII**, p. 192-202.

INTERPOL. **Financial Fraud Assessment: A global threat boosted by technology**. Disponível em: https://www.interpol.int/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology. Acesso em: 26 out. 2024.

Julio Fabbrini Mirabete, **Manual**, cit., v. 2, p. 301.

Justiça condena cuidadora a mais de sete anos de reclusão por estelionato contra idosa. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/junho/cuidadora-e-condenada-a-mais-de-sete-anos-de-reclusao-por-estelionato-contra-idosa>. Acesso em: 19 out. 2024.

LEITE, George S.; LEMOS, Ronaldo. **Marco Civil da Internet**. Rio de Janeiro: Atlas, 2014. E-book. ISBN 9788522493401. Disponível em:

https://integrada.minhabiblioteca.com.br/#/books/9788522493401/. Acesso em: 29 set. 2024.

LYRA, Roberto. Estelionato. *In:* **Repertório enciclopédico do Direito brasileiro**, Rio de Janeiro, Borsoi, s.d., v. 21, p. 53.
MIGALHAS. **Sancionadas leis que tratam de crimes cibernéticos**. 2013. Disponível em: https://www.migalhas.com.br/quentes/168701/sancionadas-leis-que-tratam-de-crimes-ciberneticos. Acesso em: 14 out. 2024.

MINAS GERAIS. Ministério Público do Estado de Minas Gerais. **Golpe do falso leilão**. Disponível em: https://www.mpmg.mp.br/portal/menu/comunicacao/publicacoes/golpe-do-falso-leilao.shtml. Acesso em: 22 out. 2024.

NORONHA, Magalhães. **Direito penal, cit., v. 2, p. 375**; Julio Fabbrini Mirabete, cit., v. 2, p. 303.

NUCCI, Guilherme de S. **Curso de Direito Penal - Vol.2.** Rio de Janeiro: Grupo GEN, 2024. E-book.Acesso em: 29 mai. 2024.

PARANÁ. Polícia Civil. **Venda intermediada por sites e golpe do falso intermediador**. Disponível em: https://www.policiacivil.pr.gov.br/NUCIBER/vendaIntermediada. Acesso em: 21 out. 2024.

PINHEIRO, Patrícia P. **Direito Digital**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9786555598438. Acesso em: 09 set. 2024.

SÃO PAULO. Polícia Civil. **Crimes cibernéticos: perguntas e respostas. Versão 2**. São Paulo: Polícia Civil, [2024]. Disponível em: https://www.policiacivil.sp.gov.br/portal/imagens/CRIMES%20CIBERN%C3%89TICOS%20-%20PERGUNTAS%20E%20RESPOSTAS%20V2.pdf. Acesso em: 24 out. 2024

SERASA EXPERIAN, 2024. **O que é phishing e como se proteger de golpes virtuais**. Disponível em: https://www.serasa.com.br/premium/blog/o-que-e-phishing/. Acesso em: 16 out. 2024.

SERASA. **Saiba como identificar um boleto falso**. 2024. Disponível em: https://www.serasa.com.br/premium/blog/boleto-falso/. Acesso em: 24 out. 2024.

STJ, **CComp 25.283/AC**, rel. Min. José Arnaldo da Fonseca, DJU, 22 nov. 1999.

SWISS SECURITY SOLUTIONS. **Interpol's Global Rapid Intervention of Payments (I-GRIP) mechanism.** Disponível em: https://www.swiss-security-solutions.com/post/interpol-s-global-rapid-intervention-of-payments-i-grip-mechanism#:~:text=3%20Min.-,Interpol's%20Global%20Rapid%20Intervention%20of%20Payments%20(I%2DGRIP

)%20mechanism,and%20recovery%20of%20illicit%20funds. Acesso em: 26 out. 2024.

TECNOBLOG. **Golpe no WhatsApp rouba conta de celular após anúncio online no OLX e Mercado Livre**. Disponível em: https://tecnoblog.net/noticias/golpe-whatsapp-rouba-conta-celular-anuncio-online-olx-mercado-livre/. Acesso em: 21 out. 2024.

The Evolution of Fraud. Disponível em: <https://www.transunion.co.uk/blog/the-evolution-of-fraud>. Acesso em: 19 out. 2024.

THREATMARK. **South Africa Online Fraud**. Disponível em: https://www.threatmark.com/south-africa-online-fraud/. Acesso em: 26 out. 2024.

Tribunal de Justiça do Distrito Federal e Territórios. **TJDFT alerta para tentativa de golpes envolvendo falsos leilões virtuais**. 2022. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2022/junho/tjdft-alerta-para-tentativa-de-golpes-envolvendo-falsos-leiloes-virtuais. Acesso em: 24 out. 2024.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SANTA CATARINA. **Golpe do falso leilão resulta na condenação de seis pessoas em Santa Catarina**. TJSC, 07 maio 2024. Disponível em: https://www.tjsc.jus.br/web/imprensa/-/golpe-do-falso-leilao-resulta-na-condenacao-de-seis-pessoas-em-santa-catarina-. Acesso em: 22 out. 2024.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. **Cuidado com golpes em falsos leilões, telefonemas, mensagens e sites**. Tribunal de Justiça do Estado de São Paulo, 30 ago. 2023. Disponível em: https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=94809. Acesso em: 22 out. 2024.

Tribunal de Justiça do Estado do Rio Grande do Sul. **Golpe do falso leilão: saiba como ocorre para se prevenir.** 2024. Disponível em: https://www.tjrs.jus.br/novo/noticia/golpe-do-falso-leilao-saiba-como-ocorre-para-se-prevenir/. Acesso em: 24 out. 2024.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Cyberfraud Industry Expands in Southeast Asia.** Disponível em: https://www.unodc.org/roseap/en/2024/10/cyberfraud-industry-expands-southeast-asia/story.html. Acesso em: 26 out. 2024.

VALKAMA, P. **A history of fraud: from ancient Egypt to the modern pandemic (Part 1)**. Disponível em: <https://www.trulioo.com/blog/fraud-prevention/history-fraud>. Acesso em: 19 out. 2024.